Department of the Army
Headquarters Fort Monroe
Fort Monroe, Virginia 23651-5000

***Fort Monroe Regulation 25-3**

7 June 2007

Information Management
INFORMATION SYSTEMS USER AND SECURITY PROCEDURES

Summary. This regulation establishes policy for managing the usage of Fort Monroe automation networks and to safeguard the use of government computer equipment from unauthorized use.

Applicability. This regulation applies to all military, civilian, and contractors located on Fort Monroe who access and use information systems.

Suggested Improvements. The proponent of this regulation is the Directorate of Information Management (DOIM). Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to US Army Garrison Fort Monroe, ATTN: IMNE-MNR-IM, 59 Patch Road, Fort Monroe, VA 23651-1052. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas For Excellence Program (AIEP) Proposal).

Availability. This regulation is only available at http://www.monroe.army.mil/Monroe/sites/publications/publications.aspx.

Contents

***This regulation supersedes FM Regulation 25-3, 17 Jan 2005 and FM Form 25-3, Apr 2006.**

1-1. Purpose. This regulation provides policy and procedures for governing the usage and protection of automated information systems (IS) and data contained on the Fort Monroe network infrastructure.

2-1. References.

a. Department of Defense Directive (DoDD) 8500.01E, Information Assurance, 24 October 2002.

b. Department of Defense Instruction (DoDI) 8500-2, IA Implementation, 6 February 2003.

c. Department of Defense(DoD) 5500.7-R, The Joint Ethics Regulation (JER), August 1993.

d. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005

e. AR 25-2, Information Assurance, 14 November 2003.

f. Memorandum, NETCOM, NETC-EST-P, 15 August 2006, subject: Army Establishes Army Golden Master (AGM) as the Standard Source for Common Operating System Baseline Configurations.

3-1. Responsibility.

a. All personnel assigned to Fort Monroe having access to the networks will comply with the provisions of this regulation.

b. Failure to comply with these policies will be reason for network access denial.

4-1. Access to the Fort Monroe Campus Area Network(CAN).

a. All DoD personnel or contractors assigned to Fort Monroe who require a network account and e-mail access will:

(1) Obtain and maintain a government common access card (CAC) for logon purposes (except volunteers and students).

(2) Read and sign a copy of the Fort Monroe AUP located at Appendix A. A signed copy of the AUP will be maintained on file with the security manager, information management officer (IMO), or supervisor as long as the user account is valid.

(4) Access and logon to Army Knowledge Online (AKO) and take the current Information Assurance Awareness computer based training (CBT) located at https://usarmy.skillport.com/SkillPortFE/login/usarmylogin.cfm.

(5) Log off all central processing units (CPU) before leaving at the end of the workday.

(6) Leave CPUs powered on allowing DOIM to update security information during non-duty hours.

b. Only government owned information systems and peripheral devices are authorized for physical connectivity to the Fort Monroe network. Personal or commercially owned information technology (IT) equipment including desktops, laptops, or printers are not authorized for connectivity to the network.

5-1. IA Awareness Training.

a. The goal of IA awareness and training is to ensure all personnel using Army information systems understand the necessity and practice of safeguarding information processed, stored, or transmitted on these systems. Annual IA training will be met through completion of the Information Assurance Awareness training located on the AKO E-learning website.

b. To meet this requirement and not cause great burden on the website, supervisors and IMOs will develop procedures to have users take their annual training during a designated month, at various intervals, or during birth months. Other procedures may be implemented as necessary to ensure compliance is met.

6-1. Deskstop application guide. In order to comply with Department of the Army(DA) guidance, workstations attaching to the Fort Monroe CAN will be installed with the current Army Gold Master (AGM) approved baseline image. This image meets regulatory and security requirements and is the DA standard.

a. The AGM baseline image is available upon request from the DOIM helpdesk. If there is no image available that meets the organization's need, the IMO or Information Assurance Security Officer (IASO) must supply DOIM with a computer hard drive in order to create an appropriate desktop installation.

b. Any changes to an image that a unit requires after initial setup must have prior written approval from the

Installation Information Assurance Manager (IAM) in order to maintain accreditation.

7-1. Consent to network monitoring. The use of DoD computer systems, including the internet, is limited to conducting official business or other authorized uses. Commanders and supervisors at all levels will educate employees on authorized and unauthorized use of government computer systems.

a. All Fort Monroe computer users consent to the monitoring of computer activity by agreeing to the DoD banner before connection to the network.

b. Inappropriate activity is defined as any use of government computer systems in a way that will reflect adversely on DoD or the Army. Listed below are examples of inappropriate activity.

(1) Content involving pornography or access to pornographic web sites.

(2) Chain-mail messages.

(3) Unofficial advertising.

(4) Soliciting or selling via e-mail.

(5) Use of pirated/illegal software.

c. The DOIM IA Office employs devices and programs to monitor the network for unusual or inappropriate activity and illegal software. When inappropriate or unauthorized software is detected emanating from a government information system, a member of the DOIM Information Assurance office will contact the user's IMO and/or Commander/Director, outlining the content found and the appropriate steps that need to be taken in order for the user and the government information system continued access to the network.

8-1. Data-at-Rest and laptop security.

a. All information systems (laptop/notebook) used for travel must be properly protected with up-to-date patches, anti-virus software and encrypted by using one of the Army approved hard drive encryption solutions. All laptops, notebooks, thumb drives, and any other data storage media must be properly marked by the organizational IMO and approved by the DOIM. No personal thumb drives are allowed on the network.

by the organizational IMO and approved by the DOIM. No personal thumb drives are allowed on the network.

b. Each individual that has the responsibility of a laptop computer should know and understand the sensitivity level of the equipment and/or data contained and must take steps to ensure its security. Laptops will not be left unattended in privately owned vehicles (POV) or government owned vehicles (GOV). Lost or stolen IT equipment, including laptops, data drives, and thumb or stick drives, must be reported immediately through their chain of command as a serious incident. Liability for the loss or theft of a laptop computer shall be evaluated in accordance with (IAW) existing policy. Failure to comply with laptop security policy constitutes negligence.

9-1. Network Equipment Policy. Non-approved networking devices are not authorized on the network. An automatic denial of service will be applied to non-compliant devices. This policy includes, but is not limited to, hubs, switches, and wireless devices found. A work order must be submitted through the Telephone Management System (TMS) if additional network cabling is required. For network device approvals and upgrades, submit a work order to monr.monroecrm@conus.army.mil.

THIS SECTION INTENTIONALLY LEFT BLANK

APPENDIX A
Sample Acceptable Use Policy

INFORMATION SYSTEMS USER AND SECURITY PROCEDURES ACCEPTABLE USE POLICY (AUP)

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the Secret Internet Protocol Router Network (SIPRNET/army.mil.) and/or Non-secure Internet Protocol Router Network (NIPRNET)/army.mil) from unauthorized or inadvertent modification, disclosure, destruction, denial or service, and use.

2. **Access.** Access to this network is for official use and authorized purposes and as set forth in DoD 5500.7-R or as further limited by this policy.

3. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. **Classified information processing.**

a. The SIPRNET is the primary classified information system for the Fort Monroe DOIM. SIPRNET is a classified only system and approved to process SECRET collateral information as SECRET and with SECRET handling instructions.

b. The SIPRNET is authorized for SECRET level processing IAW accredited SIPRNET Connection Approval File Number D960148, Identification: CCSD7184. The classification boundary between SIPRNET and NIPRNET requires vigilance and attention by all users. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. **Unclassified information processing.** NIPRNET is the primary unclassified information system for the Fort Monroe Campus Area Network. NIPRNET is an unclassified system.

a. NIPRNET provides unclassified communication to external DoD and other United States Government organizations. Primarily, this is done via e-mail and internet networking protocols such as web, ftp, and telnet.

b. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information IAW local automated information system security management policies. The garrison designated approval authority (DAA) has accredited this network for processing this type of information.

c. The NIPRNET and the internet, as viewed by the DOIM, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and internet, as well as all inbound/outbound data, external threats (e.g. worms, denial of service, hacker) and internal threats.

d. Common access card (CAC)/public key infrastructure (PKI) use.

(1) Digitally signed e-mails. As a general rule in the Army, a PKI digital signature should be used whenever e-mail is considered "official business" and contains sensitive information. The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail.

(2) Encrypted e-mails. Encrypted e-mail should be the exception, and not the rule. It should only be used to send sensitive information, information protected by the Privacy Act of 1974, and information protected under the Health Insurance Portability and Accountability Act (HIPPA).

6. Minimum security rules and requirements. As a SIPRNET and/or NIPRNET system user, the following minimum security rules and requirements apply.

a. Personnel are not permitted access to SIPRNET or NIPRNET unless in complete compliance with DoD Army personnel security requirements for operating in a SECRET system-high environment.

b. I will generate, store, and protect pin numbers, passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases) IAW AR 25-2, passwords should be changed at least every 90 days.

c. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

d. To protect the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb storage device, or other storage media.

e. I will not attempt to access or process data exceeding the authorized information system classified level.

f. I will not alter, change, configure, or use operating system or programs, except as specifically authorized.

g. I will not introduce executable codes (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious codes.

h. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

i. I will not utilize Army or DoD provided information systems for commercial financial gain or illegal activities.

j. Maintenance will be performed by the system administrator (SA) only.

k. I will use screen locks and logoff the workstation when departing the area.

l. I will immediately report any suspicious output, files, shortcuts, or phishing attempts to the SA and/or the IASO and cease all activities on the system. The Monroe Helpdesk should be contacted at 788-3055 or forward an e-mail message to monr.monroecrm@conus.army.mil for assistance and to report any classified spillage. The classified spillage will be reported to the Fort Monroe Security Officer and Network Managers for action.

m. I will address any questions regarding policy, responsibilities, and duties to my security manager.

n. I understand that each information system is the property of the Army and is provided to me for official and authorized use. I further understand that each information system is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the information system and may have only a limited expectation of privacy in personal data. I realize that I should not store data on the information system that I do not want others to see

o. I understand that monitoring of SIPRNET and NIPRNET will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions. I understand that the following activities are prohibited uses of an Army information system:

(1) Unethical use (e.g. spam, profanity, sexual misconduct, gaming, extortion).

(2) Entering and showing unauthorized sites (e.g. pornography, streaming videos, chat rooms).

(3) Entering and showing unauthorized services (e.g. peer-to-peer, distributed computing).

(4) Unacceptable use of e-mail include exploiting list servers or similar group broadcast systems for purposes beyond intended scope to widely distribute unsolicited e-mail; sending the same e-mail message repeatedly to interfere with recipient's use of e-mail; sending or broadcasting, e-mail messages of quotations, jokes, etc., to multiple addressees; sending or broadcasting unsubstantiated virus warnings from sources other than IAMs (e.g. mass mailing, hoaxes, auto-forwarding).

(5) Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).

(6) To show what is deemed proprietary or not releasable (e.g. use of keywords, phrases or data identification).

p. I understand that I may use an Army information system for limited personal communications by e-mail and brief internet searches provided they are before or after duty hours, break periods or lunch time, as long as they do not cause an adverse impact on the employee's official duties; are of reasonable duration, and cause no adverse reflection on DoD. Unacceptable use of services or policy violations may be a basis for disciplinary actions and denial of services for any user.

q. I will participate in all user training programs as required to support the annual training requirement (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

r. The authority for soliciting your social security number (SSN) is Executive Order 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to the Fort Monroe Campus Area Network information system.

7. Acknowledgement. I have read the above requirements regarding use of the Fort Monroe NIPRNET and SIPRNET access systems. I understand my responsibilities regarding these systems and the information contained in them. I understand this signed agreement will be kept, on file, by the staff's security manager. I have completed the Information Assurance Awareness Training located on the AKO E-Learning website at https://usarmy.skillport.com/SkillPortFE/login/usarmylogin.cfm and have provided the certificate of completion to the security manager or IMO.

____

Directorate/Division/Branch

____

Last Name, First, MI (print)

____

Rank/Grade and SSN (last 4 digits)

____

Signature and Date

____

Security Manager/IMO and Date

REQUEST FOR FORT MONROE CAMPUS AREA NETWORK (CAN) ACCESS

Privacy Act Statement

Authority. 5 U.S.C. 301 and E.O. 9397(SSN). **Principal Purpose.** Information will be used to establish access to the installations campus area network. **Routine Use.** Information is required by the Directorate of Information Management (DOIM), Fort Monroe. Data will remain on file for ninety (90) days. **Disclosure.** Voluntary; however, failure to provide requested information will result in denial of campus area network access.

Employee Information

Name ____________________ SSN ____________

Last *First* *MI*

○ Military ○ Civilian ○ DA Intern Rank/Grade ________ □ Contractor Company Name ____________

Administrative Office

Directorate ____________ Division ____________ Branch ____________

Office Symbol ____________ Bldg # ______ Rm # ______ Telephone # ____________

Position Title ____________________

ID/Add Employee to the following e-mail distribution lists: ____________________

POC Name ____________ Telephone ____________ Fax ____________

Administrative Office/IMO

TRADOC Electronic Personnel Locator (TEPL) System ____________________

Employee AKO User ID ____________________ @us.army.mil

(Employee must have a valid AKO account. For more information about creating a new AKO account, visit www.us.army.mil)

Security Manager

Initial Security Briefing ____________ Issue Bldg Keys ○ Yes ○ No

(AR 380-5, Para 9-3) *(Date)*

Initial IA Briefing ____________ Initiate CAC Card ○ Yes ○ No

(AR 25-2, Para 4-3) *(Date)*

Have user read and sign FM Memorandum 25-2

Background Investigation

(See AR 25-2, para 4-14 for IT requirement)

Investigation Type ____________ Date Investigation Closed ____________ (IT-III)

Security Clearance Level ____________ Eligibilitiy Date ____________ (IT-I or II)

Investigation Initiated/Favorable Review: Type ____________ Date ____________

Local Records Check Date ____________ Security Manager Signature ____________________

If employee has no investigative information on file, contact Garrison Security at 788-3669/2699 to initiate SF 85P or SF 86 (AR 380-67)

FM Form 25-3, 5 Feb 2007

HELP DESK/IMO

Add TEPL Userid

ID Active Directory Organizational Unit

Assign IT Equipment ○ Yes ○ No Help Desk Configure Equipment ○ Yes ○ No

Computer Model

Serial Number

Monitor Model

Serial Number

Computer Name

Add to the following e-mail distribution lists

Fax completed form to 757-788-3328

FM Form 25-3, 5 Feb 2007

Print Form

GLOSSARY

AGM	Army Golden Master
AIS	Automated Information System
AKO	Army Knowledge Online
AR	Army Regulation
AUP	acceptable use policy
CAC	common access card
CAN	campus area network
CPU	central processing unit
DAA	designating approval authority
DAR	data-at-rest
DoD	Department of Defense
DOIM	Directorate of Information Management
GOV	Government owned vehicle
HIPPA	Health Insurance Portability and Accountability Act
IA	information assurance
IASO	Information Assurance Security Officer
IAM	Information Assurance Manager
IAW	in accordance with
IMO	Information Management Officer
IT	information technology
NIPRNET	non-secure internet protocol router network
PKI	public key infrastructure
POV	privately owned vehicle
SA	system administrator
SIPRNET	secret internet protocol router network
SSN	social security number

JASON T. EVANS
Colonel, Adjutant General
Commanding

DISTRIBUTION:
http://www.monroe.army.mil/Monroe/sites/publications/publications.aspx